

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-051816

(43)Date of publication of application : 21.02.2003

(51)Int.Cl.  
H04L 9/08  
G06F 17/60  
G09C 1/00  
H04N 7/08  
H04N 7/081  
H04N 7/16  
// H04N 7/167

(21)Application number : 2001-239148

(71)Applicant : SONY CORP

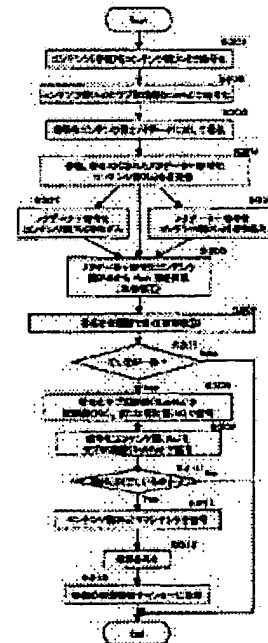
(22)Date of filing : 07.08.2001

(72)Inventor : SATO HIDEO  
KATO ARIYOSHI

(54) CONTENTS DISTRIBUTION SYSTEM, CONTENTS DISTRIBUTION METHOD, DATA PROCESSOR, DATA PROCESSING METHOD, AND COMPUTER PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents distribution system for distributing encrypted contents which can effectively exclude illegal use of contents.  
SOLUTION: The system that distributes encrypted contents and allows only legal users to utilize the contents is configured such that a contents management distribution site for distributing contents generates a hash value of data incorporating meta data containing contents cost information and a contents key applied to contents encryption processing and executes an electronic signature, a user site receiving the data acquires the contents key stored in signature object data on the condition that signature verification is established, and the system can prevent illegal use of contents through falsification or replacement of the meta data.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-51816  
(P2003-51816A)

(43) 公開日 平成15年2月21日 (2003. 2. 21)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
H 0 4 L 9/08		G 0 6 F 17/60	3 3 2 5 C 0 6 3
G 0 6 F 17/60	3 3 2	G 0 9 C 1/00	6 4 0 B 5 C 0 6 4
G 0 9 C 1/00	6 4 0		6 4 0 Z 5 J 1 0 4
		H 0 4 N 7/16	C
H 0 4 N 7/08		H 0 4 L 9/00	6 0 1 B

審査請求 未請求 請求項の数21 OL (全 24 頁) 最終頁に続く

(21) 出願番号 特願2001-239148(P2001-239148)

(22) 出願日 平成13年8月7日 (2001. 8. 7)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 佐藤 英雄

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72) 発明者 加藤 有美

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

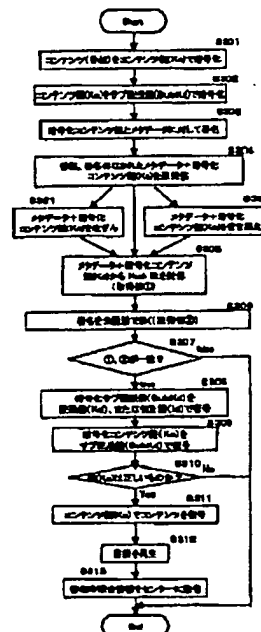
最終頁に続く

(54) 【発明の名称】 コンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラム

(57) 【要約】

【課題】 暗号化コンテンツを配信するシステムにおいて、コンテンツの不正利用の効果的排除を可能としたコンテンツ配信システムを実現する。

【解決手段】 暗号化コンテンツの配信を行ない、正規ユーザにおいてのみコンテンツの利用を許容するシステムにおいて、コンテンツ配信を行なうコンテンツ管理配信サイトにおいて、コンテンツの価格情報を含むメタデータと、コンテンツの暗号処理に適用するコンテンツ鍵を併せたデータのハッシュ値を生成して電子署名を実行し、データを受信したユーザサイトにおいて、署名検証の成立を条件として署名対象データ中に格納されたコンテンツ鍵の取得を可能とする構成とし、メタデータ改竄、あるいは置き換えによるコンテンツ不正利用を防止可能とした。



【特許請求の範囲】

【請求項1】コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信システムにおいて、前記コンテンツ配信サイトは、

コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行する構成を有し、

前記ユーザサイトは、

前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ配信システム。

【請求項2】前記ユーザサイトは、

前記電子署名の検証処理として、

前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、

前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行する構成であり、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成であることを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項3】前記メタデータは、コンテンツの利用価格情報を含み、

前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項4】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵(SubKd)であり、

前記コンテンツ配信サイトは、前記サブ配送鍵(SubKd)を配送鍵(Kd)で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、

前記ユーザサイトは、

前記電子署名の検証成立を条件として、予め保有する前記配送鍵(Kd)を用いた復号処理により、前記サブ配送鍵(SubKd)の取得処理を実行し、前記サブ配送鍵(SubKd)を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項5】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵(SubKd)であり、

前記コンテンツ配信サイトは、前記サブ配送鍵(SubKd)を、各ユーザサイトに個別に配布された個別鍵

(Ki)で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、

前記ユーザサイトは、

前記電子署名の検証成立を条件として、予め保有する前記個別鍵(Ki)を用いた復号処理により、前記サブ配送鍵(SubKd)の取得処理を実行し、前記サブ配送鍵(SubKd)を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項1に記載のコンテンツ配信システム。

【請求項6】コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信方法であり、

前記コンテンツ配信サイトにおいて、

コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行し、

前記ユーザサイトにおいて、

前記電子署名の検証処理を実行し、該電子署名検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするコンテンツ配信方法。

【請求項7】前記ユーザサイトは、

前記電子署名の検証処理として、

前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、

前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする請求項6に記載のコンテンツ配信方法。

【請求項8】前記メタデータは、コンテンツの利用価格情報を含み、

前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行することを特徴とする請求項6に記載のコンテンツ配信方法。

【請求項9】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵(SubKd)であり、

前記コンテンツ配信サイトは、前記サブ配送鍵(SubKd)を配送鍵(Kd)で暗号化した鍵データをユーザサイトに送信する処理を実行し、

前記ユーザサイトは、

前記電子署名の検証成立を条件として、予め保有する前記配送鍵(Kd)を用いた復号処理により、前記サブ配送鍵(SubKd)の取得処理を実行し、前記サブ配送鍵(SubKd)を用いた復号処理により、コンテンツ

鍵を取得することを特徴とする請求項6に記載のコンテンツ配信方法。

【請求項10】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（SubKd）であり、

前記コンテンツ配信サイトは、前記サブ配送鍵（SubKd）を、各ユーザサイトに個別に配布された個別鍵（Ki）で暗号化した鍵データをユーザサイトに送信する処理を実行し、

前記ユーザサイトは、

前記電子署名の検証成立を条件として、予め保有する前記個別鍵（Ki）を用いた復号処理により、前記サブ配送鍵（SubKd）の取得処理を実行し、前記サブ配送鍵（SubKd）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする請求項6に記載のコンテンツ配信方法。

【請求項11】暗号化コンテンツの復号処理を実行するデータ処理装置であり、

コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するデータ処理手段を有することを特徴とするデータ処理装置。

【請求項12】前記データ処理手段は、

前記電子署名の検証処理として、

前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、

前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とする請求項11に記載のデータ処理装置。

【請求項13】前記データ処理装置は、

前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする請求項11に記載のデータ処理装置。

【請求項14】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（SubKd）であり、

前記データ処理装置は、

前記電子署名の検証成立を条件として、予め保有する配送鍵（Kd）を用いた復号処理により、前記サブ配送鍵（SubKd）の取得処理を実行し、前記サブ配送鍵（SubKd）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項11に記載のデータ処理装置。

【請求項15】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（SubKd）であり、

前記データ処理装置は、

前記電子署名の検証成立を条件として、予め保有する個別鍵（Ki）を用いた復号処理により、前記サブ配送鍵（SubKd）の取得処理を実行し、前記サブ配送鍵（SubKd）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項11に記載のデータ処理装置。

【請求項16】暗号化コンテンツの復号処理を実行するデータ処理方法であり、

コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするデータ処理方法。

【請求項17】前記電子署名の検証処理は、

前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、

前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理であり、

該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする請求項16に記載のデータ処理方法。

【請求項18】前記データ処理方法は、さらに、

前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行することを特徴とする請求項16に記載のデータ処理方法。

【請求項19】前記データ処理方法において、

前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（SubKd）であり、

前記電子署名の検証成立を条件として、予め保有する配送鍵（Kd）を用いた復号処理により、前記サブ配送鍵（SubKd）の取得処理を実行し、前記サブ配送鍵（SubKd）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする請求項16に記載のデータ処理方法。

【請求項20】前記データ処理方法において、

前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（SubKd）であり、

前記電子署名の検証成立を条件として、予め保有する個別鍵（Ki）を用いた復号処理により、前記サブ配送鍵（SubKd）の取得処理を実行し、前記サブ配送鍵（SubKd）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする請求項16に記載のデータ処理方法。

【請求項21】暗号化コンテンツの復号処理を含むデータ処理をコンピュータ・システム上で実行せしめるコン

ビュータ・プログラムであって、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行するステップと、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するステップと、を具備することを特徴とするコンピュータ・プログラム。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、コンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムに関する。特に、暗号化されたコンテンツを配信するシステムにおいて、コンテンツの価格情報等を含むメタデータの改竄、置き換えなどによるコンテンツの不正利用を防止するコンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムに関する。

##### 【0002】

【従来の技術】昨今、音楽データ、画像データ、ゲームプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット、衛星を介した通信他、有線、無線の各種通信網を介して配信するサービスが盛んになってきている。また、DVD、CD、メモリカード等の流通可能な記憶媒体を介したコンテンツ流通も盛んになってきている。これらの流通コンテンツは、ユーザの所有する例えば、TV、PC（Personal Computer）、再生専用器、あるいはゲーム機器等において、再生、利用される。

【0003】通信網を介して配信されるコンテンツは、例えば通信機能を有するセットトップボックスによって受信され、TV他の再生装置において再生可能なデータに変換されて再生される。あるいは通信インタフェースを備えたTV、再生装置、ゲーム機器、PC等の情報機器によって受信されて再生される。

【0004】ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0005】ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。例えば著作権保護の要請されるコンテンツを衛星あるいはインターネット等を介して配信する場合にコンテンツを暗号化

して配信し、正規ユーザに対してのみ復号鍵を配布する。正規ユーザは配布された復号鍵によって暗号化コンテンツの復号を実行し、コンテンツを再生する構成である。

【0006】例えば、正規ユーザに対して暗号化コンテンツを復号するための鍵を格納したメモリ媒体（例えばICカード）を配布し、ユーザは配布されたICカードをセットトップボックスまたは受信機にセットし、セットしたカードの格納鍵を用いて暗号化コンテンツの復号処理を実行して再生する構成がある。

【0007】図1を用いて、コンテンツをコンテンツ鍵で暗号化して配信するコンテンツ配信システム構成例について説明する。

【0008】図1は、コンテンツ（番組）を制作または提供するコンテンツ提供サイト10と、コンテンツを受信して再生するユーザサイト20における処理を説明する図である。管理センター30は、配送鍵（Kd：Distribution Key）をコンテンツ提供サイト10とユーザサイト20に提供する。ユーザサイト20には、例えばデータの取り出しを防止したセキュアモジュールとしてのICカード内に配送鍵（Kd）を格納して提供する。

【0009】図1に示す番号（1）～に沿って処理が行われる。処理の詳細について説明する。まず、コンテンツ提供サイト10では、（1）コンテンツを暗号化するためのコンテンツ鍵（Kc）を生成し、（2）生成したコンテンツ鍵（Kc）を用いてコンテンツの暗号化処理を実行する。暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、例えば代表的な共通鍵暗号アルゴリズムであるDES（Data Encryption Standard）が適用できる。

【0010】共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な暗号化方式がDES（データ暗号標準：Data encryption standard）である。

【0011】さらに、安全性を増すためにDESアルゴリズムを3重にして処理を行なうトリプルDESを適用してもよい。DES暗号化処理では鍵長56ビットの鍵を生成してコンテンツ鍵として使用し、トリプルDESでは112ビットの鍵長を持つ鍵をコンテンツ鍵として生成する。このようなコンテンツ鍵は、乱数発生装置において発生した乱数に基づいて生成するものであり、コンテンツ毎に生成する。

【0012】コンテンツ提供サイト10は、生成したコンテンツ鍵（Kc）を用いてコンテンツを暗号化するとともに、（3）生成したコンテンツ鍵（Kc）を管理センター30から受領した配送鍵（Kd）を用いて暗号化する。この場合の暗号化アルゴリズムもやはりDESや

トリプルDESなどの共通鍵アルゴリズムが用いられる。さらに暗号化コンテンツ鍵(Kc)にコンテンツの利用条件、すなわちコピーしてよいか、あるいは価格などの付加情報によって構成されるメタデータを付加する。さらに、コンテンツ提供サイト10は、メタデータの改竄防止のためにメタデータのハッシュ(Hash)値を算出し、ハッシュ値に対してコンテンツ提供サイト10の秘密鍵を用いて電子署名を施す。

【0013】コンテンツ提供サイト10は、(4)コンテンツ鍵(Kc)で暗号化したコンテンツと、配送鍵(Kd)で暗号化したコンテンツ鍵(Kc)と、署名を施したメタデータ、さらに、コンテンツ提供サイト10の公開鍵証明書をユーザに向けて配信する。これらのデータは共に衛星、インターネットなどの配信経路を通じてユーザサイト20の受信機に送られ、例えば受信機内のHDDなどの蓄積装置に蓄積される。

【0014】ユーザサイト20では、まず、(5)受信したメタデータに対する署名検証を行なう。まず、コンテンツ提供サイト10の公開鍵証明書を、ユーザサイト20に予め配布されている認証局の公開鍵で検証し、公開鍵証明書からコンテンツ提供サイト10の公開鍵を取り出し、取り出したコンテンツ提供サイト10の公開鍵によって署名検証を実行する。

【0015】ユーザは、購入条件を確認して購入を決定すると、(6)管理センター30から受領した配送鍵(Kd)を用いて暗号化コンテンツ鍵(Kc)の復号を行なう。配送鍵(Kd)は、前述したように正しい契約が行われた受信機または、受信機に装着されたカードモジュールなどの安全なモジュール内に格納されている。

【0016】暗号化されたコンテンツ鍵が受信機内で配布鍵によって復号化されると、利用条件に基づき、

(7)コンテンツ鍵を用いてコンテンツが復号されて再生される。さらに、再生と同時に課金ログを生成し、生成した課金ログをこの配信サービスを行うための管理センター30に送信し決済を行う構成とすることができる。

【0017】管理センター30は配送鍵(Kd)の管理、ユーザサイト20の受信機あるいはカードモジュールの管理、顧客管理を行う。管理センター30とユーザサイト20の受信機あるいはカードモジュールとは電話回線などの下回線を通じて、一定期間毎に通信を行い、相互認証を行って配送鍵(Kd)の配布処理、および課金ログの回収処理を行う。

【0018】図1の構成のように、コンテンツの暗号化はコンテンツの配信事業者または番組制作者としてのコンテンツ提供サイト10が行うのが一般的で、コンテンツ提供サイト10の暗号化装置に管理センターが管理している配送鍵(Kd)を入力することでコンテンツ提供サイト10が暗号化コンテンツ鍵を生成する。管理センター30は、正規ユーザであるユーザサイト20に対し

ても暗号化コンテンツ鍵を復号するための配送鍵(Kd)を提供する。このように、管理センター30は配送鍵(Kd)の管理および提供によりコンテンツの配信管理、課金処理を行なっている。

【0019】また、CSあるいはBS放送等、衛星を用いたコンテンツ配信においては、フラット課金、すなわち月極めの一定料金で有料番組が視聴できる形態としたサービスも存在する。この場合には、視聴が許された受信機あるいはカードモジュールに対応して各々異なる個別鍵を設定する。放送局は、設定したすべての個別鍵で暗号化コンテンツ鍵を暗号化してコンテンツと共に衛星から配布する。この構成の場合も、すべての個別鍵が管理センターから配信事業者あるいは番組制作者に渡され、コンテンツ鍵が暗号化される。このようなシステム具体例として、CSあるいはBSデジタル放送で採用されているCAS(Conditional Access System)がある。

【0020】CAS(Conditional Access System)は、配信番組(コンテンツ)をスクランブル処理し、スクランブルを解くための鍵(スクランブル鍵:Ksc)を番組とともに、番組付帯情報として送信する。正規ユーザには、ICカードが予め配布される。ICカードには、暗号化されたスクランブル鍵(Ksc)を復号するためのワーク鍵(Kwk)が格納される。

【0021】ただしワーク鍵(Kwk)を固定化すると、鍵の漏洩の可能性があるので、ワーク鍵(Kwk)は定期的に更新する。更新時には更新されたワーク鍵(Kwk)を暗号化して配信する。ユーザに対して送信するスクランブル鍵(Ksc)は、コンテンツ番組情報を含むECM(Entitlement Control Message)内に含ませて放送データとして送信する。また、ワーク鍵(Kwk)は、各ユーザに渡されているICカードの識別子(ID)を付加情報として持つEMM(Entitlement Management Message)に含ませて放送波で送信する。

【0022】暗号化されたワーク鍵は、正規ユーザに配布されているICカードに格納されたマスタ鍵(Km)を用いることによって復号可能となる。ICカードに格納されたマスタ鍵(Km)は、各ICカード毎に異なる固有の鍵(個別鍵)である。

【0023】マスタ鍵(Km)は各ICカードに固有の鍵であるため、更新されたワーク鍵(Kwk)を暗号化して配信する場合には、正規ユーザの受信機の数(=マスタ鍵の数)に対応する数の暗号化ワーク鍵を配信する。配信する複数の暗号化ワーク鍵の各々にはICカード各々に対応したID番号が付与されており、受信機側では、自己のICカードに一致するIDを持つ暗号化ワーク鍵データを選択して、ICカードに格納されたマスタ鍵(Km)を適用した復号処理を実行してワーク鍵を取得する。

【0024】ユーザは取得したワーク鍵(Kwk)を用いてスクランブルコンテンツ(番組)とともに配信され

た暗号化スクランブル鍵(Ks)の復号処理を実行して、スクランブル鍵(Ks)を取得して、取得したスクランブル鍵(Ks)を用いてスクランブルコンテンツ(番組)のスクランブル解除(デスクランブル)処理を実行してコンテンツ(番組)を再生する。

【0025】

【発明が解決しようとする課題】上記のようなコンテンツ配信システムにおいて、コンテンツの利用条件、すなわちコピーしてよいか、あるいは価格などの付加情報によって構成されるメタデータを暗号化コンテンツ鍵とともに送信する際、コンテンツ提供サイト10は、メタデータの改竄防止のためにメタデータのハッシュ(Hash)値を算出し、ハッシュ値に対してコンテンツ提供サイト10の秘密鍵を用いて電子署名を施していた。

【0026】ユーザサイトでは、受信したメタデータから計算したハッシュ(Hash)値と、署名を公開鍵を適用した復号処理により解いて取得される復号値としてのハッシュ(Hash)値を比較して、一致したら改竄なしと判定し、利用条件を確認した後、配送鍵(Kd)やワーク鍵(Kw)を適用した復号処理を実行可能としてコンテンツ鍵の取り出し、コンテンツを利用していた。

【0027】しかし、従来の構成では、あるコンテンツに対応した価格情報を設定しているメタデータを他のコンテンツに対応付けるなどの処理により、例えば、値段の高い番組情報と、値段の安い番組情報のすりかえを行ない、安い値段のコンテンツに対応するメタデータを高い番組の再生に利用するなどの不正が発生する可能性があった。

【0028】従来のメタデータの署名検証処理、コンテンツ利用について図2を用いて説明する。コンテンツ提供サイト(センター)は番組Aをコンテンツ鍵(Kc-a)で暗号化し、番組Aの価格情報を含むメタデータのハッシュ値をコンテンツ提供サイトの秘密鍵(Ks)による暗号化処理で署名を生成し、これらをユーザサイトに送信する。ユーザサイト側は、コンテンツ提供サイト(センター)の秘密鍵(Ks)に対応する公開鍵を公開鍵証明書から取り出して、公開鍵を適用して署名を解いて取得した値と、メタデータから計算したハッシュ(Hash)値とが一致しているかどうかのチェックを行う。一致していれば、購入条件等のメタデータが改ざんされていないものとして、上述の配送鍵または個別鍵等の鍵(Kw)で暗号化コンテンツ鍵(Kc-a)を復号してコンテンツ鍵(kc-a)を取得し、取得したコンテンツ鍵(Kc-a)を使用して番組Aを再生することが可能となる。番組Bについても、全く同様の処理により、コンテンツ鍵(kc-b)を取得し、取得したコンテンツ鍵(Kc-b)を使用して番組Bの再生が可能となる。

【0029】一方、メタデータの改竄、置き換えによる

不正なコンテンツ利用例について図3を参照して説明する。図3(a)に示すように、例えば300円の番組Aを100円で見ようと、メタデータを改竄した場合。改竄したメタデータからハッシュ(Hash)値を計算したものは、コンテンツ提供サイト(センター)から送られてきたハッシュ(Hash)値と異なる。両者が一致しないので、再生することは不可能である。

【0030】しかし、図3(b)に示すように、例えば1000円の番組Bを見るために、300円の番組Aのメタデータと署名を不正に利用する。まず、ユーザは、300円の番組Aのメタデータについての署名検証を1000円の番組Bに対応する処理として実行する。この場合、番組Aのメタデータからハッシュ(Hash)値を計算したものと、番組Aを購入した際にコンテンツ提供サイト(センター)から送られてきた番組Aのハッシュ(Hash)値は、本来番組Bのものではないが、番組Bのものとして両方とも番組Aから置き換えられたものなので、一致してしまう。一致したことが証明されれば、そこでシステムは、次のステップの処理への移行を許可してしまう。次ステップでは、配送鍵または個別鍵等の固有の鍵(Kw)で暗号化コンテンツ鍵(Kc-b)を復号してコンテンツ鍵(kc-b)を取得し、取得したコンテンツ鍵(Kc-b)を使用して番組Bを再生することが可能となる。その際、管理センターに送られる課金情報は置きかえられたメタ情報である番組Aの300円になってしまう。

【0031】従来のシステムにおける署名検証処理に基づくコンテンツ(番組)再生処理との対応について図4を用いて説明する。ユーザサイトの例えばセットトップボックス等のシステムでは、メタデータからハッシュ(Hash)値を計算し、また、コンテンツ提供サイト(センター)の秘密鍵(Ks)に対応する公開鍵を公開鍵証明書から取り出して、署名をコンテンツ提供サイトの公開鍵で解いて得たハッシュ(Hash)値との比較を実行する。この比較において一致と判定されると、購入条件等のメタデータが改ざんされていないものと判断され、次の処理ステップへの移行が許可される。

【0032】署名検証成功によって実行可能となる処理ステップは、配送鍵または個別鍵等の固有の鍵(Kw)で暗号化コンテンツ鍵(Kc)を復号してコンテンツ鍵(kc)を取得し、取得したコンテンツ鍵(Kc)を使用して番組を再生する処理である。メタデータが番組Aに対応するものであれば、番組Aのコンテンツ鍵(Kc-a)の取得および番組Aの再生は、正当利用であるが、メタデータが番組Aに対応するにもかかわらず、ハッシュ値の一致を条件として番組Bのコンテンツ鍵(Kc-b)の取得および番組Bの再生を可能とする処理も可能であり、不正なコンテンツ利用が行われる恐れがある。

【0033】図5に、メタデータの置き換えによりコン

テンツの不正利用を行なう場合の手順を説明するフローを示す。各ステップについて説明する。ステップS101で、コンテンツ提供サイト（センター）は番組Bを、コンテンツ鍵（Kc）で暗号化し、ステップS102で、番組Bのメタデータ、センターの秘密鍵（Ks）で暗号化された署名と共にユーザサイトに対して送信する。

【0034】ユーザサイトでは、送信されてきた番組Bを再生するために、ステップS103で、番組Bのメタデータと送信された署名を番組Aのメタデータと送信された署名に置き換える。ステップS104で置き換えられた番組Aのメタデータからハッシュ（Hash）値を計算する（取得値を①とする）。次にステップS105で、署名部分（こちらも置き換えられた番組Aの署名）をセンターの公開鍵で解く（取得値を②とする）。ステップS106で、①と②が一致しているかどうかの判断を行う。この場合、両方とも置き換えられたもので、一致する。一致したことが証明されれば、そこで再生許可が出てしまうので、ステップS107で、番組Bが再生可能となってしまう。そして、番組Bを再生したにもかかわらず、ステップS108で、番組Aの課金情報が管理センターに送られる。

【0035】次に、ユーザサイト側のシステム、例えばセットトップボックス、再生装置等で実行されるハッシュ（Hash）値の照合処理の手順について図6のフローチャートを用いて説明する。ステップS201で、メタデータからハッシュ（Hash）値を計算する（取得値を①とする）。ステップS202で、送信されてきた署名を、公開鍵証明書から取り出した公開鍵を適用して解く（取得値を②とする）。ステップS203で、各取得値①と②が一致しているかどうかの判断を行う。一致していたら、ステップS204で、番組Aに対応する暗号化コンテンツ鍵を配送鍵（Kd）または個別鍵（Kw）を適用した復号処理により、コンテンツ鍵（Kc）を取得する。ステップS205で、取得したコンテンツ鍵（Kc）で番組Aを再生することが可能となる。さらに、ステップS206で、メタ情報に記録された課金情報がセンターに送られる。

【0036】このように、従来のコンテンツ配信システムでは、コンテンツの利用条件、価格などの付加情報によって構成されるメタデータを送信する際、メタデータについてのハッシュ値生成、署名処理を実行し、ユーザサイトでは、受信した署名の検証成立により、コンテンツ鍵の取得ステップを実行する構成であり、署名検証対象のメタデータと、復号処理対象となる暗号化コンテンツ鍵との関連付けがなされていないため、あるコンテンツに対応しているメタデータについての署名検証に基づいて他のコンテンツに対応したコンテンツ鍵の取得処理を実行して不正にコンテンツを再生、利用するという事態が発生していた。

【0037】本発明は、上述の問題点に鑑みてなされたものであり、署名検証処理を実行した正当な対応コンテンツをのみ利用可能な構成を実現し、不正なコンテンツ利用を排除可能としたコンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0038】

【課題を解決するための手段】本発明の第1の側面は、コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信システムにおいて、前記コンテンツ配信サイトは、コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行する構成を有し、前記ユーザサイトは、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ配信システムにある。

【0039】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザサイトは、前記電子署名の検証処理として、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行する構成であり、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成であることを特徴とする。

【0040】さらに、本発明のコンテンツ配信システムの一実施態様において、前記メタデータは、コンテンツの利用価格情報を含み、前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする。

【0041】さらに、本発明のコンテンツ配信システムの一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（SubKd）であり、前記コンテンツ配信サイトは、前記サブ配送鍵（SubKd）を配送鍵（Kd）で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記配送鍵（Kd）を用いた復号処理により、前記サブ配送鍵（SubKd）の取得処理を実行し、前記サブ配送鍵（SubKd）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【0042】さらに、本発明のコンテンツ配信システム



の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵 (SubKd) であり、前記コンテンツ配信サイトは、前記サブ配送鍵 (SubKd) を、各ユーザサイトに個別に配布された個別鍵 (Ki) で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記個別鍵 (Ki) を用いた復号処理により、前記サブ配送鍵 (SubKd) の取得処理を実行し、前記サブ配送鍵 (SubKd) を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【0043】さらに、本発明の第2の側面は、コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信方法であり、前記コンテンツ配信サイトにおいて、コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行し、前記ユーザサイトにおいて、前記電子署名の検証処理を実行し、該電子署名検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするコンテンツ配信方法にある。

【0044】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザサイトは、前記電子署名の検証処理として、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする。

【0045】さらに、本発明のコンテンツ配信方法の一実施態様において、前記メタデータは、コンテンツの利用価格情報を含み、前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行することを特徴とする。

【0046】さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵 (SubKd) であり、前記コンテンツ配信サイトは、前記サブ配送鍵 (SubKd) を配送鍵 (Kd) で暗号化した鍵データをユーザサイトに送信する処理を実行し、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記配送鍵 (Kd) を用いた復号処理により、前記サブ配送鍵 (SubKd) の取得処理を実行し、前記サブ配送鍵 (SubKd) を

用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【0047】さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵 (SubKd) であり、前記コンテンツ配信サイトは、前記サブ配送鍵 (SubKd) を、各ユーザサイトに個別に配布された個別鍵 (Ki) で暗号化した鍵データをユーザサイトに送信する処理を実行し、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記個別鍵 (Ki) を用いた復号処理により、前記サブ配送鍵 (SubKd) の取得処理を実行し、前記サブ配送鍵 (SubKd) を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【0048】さらに、本発明の第3の側面は、暗号化コンテンツの復号処理を実行するデータ処理装置であり、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するデータ処理手段を有することを特徴とするデータ処理装置にある。

【0049】さらに、本発明のデータ処理装置の一実施態様において、前記データ処理手段は、前記電子署名の検証処理として、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とする。

【0050】さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする。

【0051】さらに、本発明のデータ処理装置の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵 (SubKd) であり、前記データ処理装置は、前記電子署名の検証成立を条件として、予め保有する配送鍵 (Kd) を用いた復号処理により、前記サブ配送鍵 (SubKd) の取得処理を実行し、前記サブ配送鍵 (SubKd) を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【0052】さらに、本発明のデータ処理装置の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵 (SubKd) であり、前記データ処理装置は、前記電子署名の検証成立を条件として、予め保有する個別鍵 (Ki) を用いた復号処理により、前記サブ配送鍵 (SubKd) の取得処理を実行し、前記サブ配送鍵

(SubKd)を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【0053】さらに、本発明の第4の側面は、暗号化コンテンツの復号処理を実行するデータ処理方法であり、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするデータ処理方法にある。

【0054】さらに、本発明のデータ処理方法の一実施態様において、前記電子署名の検証処理は、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理であり、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする。

【0055】さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法は、さらに、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行することを特徴とする。

【0056】さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵(SubKd)であり、前記電子署名の検証成立を条件として、予め保有する配送鍵(Kd)を用いた復号処理により、前記サブ配送鍵(SubKd)の取得処理を実行し、前記サブ配送鍵(SubKd)を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【0057】さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵(SubKd)であり、前記電子署名の検証成立を条件として、予め保有する個別鍵(Ki)を用いた復号処理により、前記サブ配送鍵(SubKd)の取得処理を実行し、前記サブ配送鍵(SubKd)を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【0058】さらに、本発明の第5の側面は、暗号化コンテンツの復号処理を含むデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行するステップと、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するステップと、を具備することを特徴とするコンピュータ・プ

ログラムにある。

【0059】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0060】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集積構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0061】

【発明の実施の形態】  
【システム概要】図7に本発明のコンテンツ配信システムを実現するシステム構成例を示す。図7において、コンテンツは、コンテンツ配信管理サイト200のコンテンツ配信部(例えば放送局)230において暗号化(スクランブル処理も含む)されてコンテンツ配信部230から通信衛星、インターネット等の各種通信手段を介してユーザサイト100の受信手段(例えばSTB:セットトップボックス)120に向けて配信される。

【0062】ユーザサイト100の受信手段120は、コンテンツ配信部230からの配信データを受信する通信インタフェースを備える。配信データ中のコンテンツは暗号化されており、所定の鍵を用いた復号処理を実行した後、TV等の出力手段140において出力される。コンテンツデータの復号処理等を実行するのは、データ処理手段110である。データ処理手段110と受信装置120間は例えばIEEE1394インタフェースによって接続される。

【0063】データ処理手段110は、受信コンテンツの蓄積用記憶装置として例えばHDDを有し、さらにコンテンツの復号処理などを実行する暗号処理部としてのセキュアモジュール115を有する。セキュアモジュール115は、署名検証処理、暗号化コンテンツの復号処理を実行する暗号処理機能を持ち、暗号処理に適用する鍵の格納領域を有する。さらに、サービス管理センタ300からの鍵配信処理の際の相互認証処理を実行する。

【0064】コンテンツ配信部230によって配信されるコンテンツは、コンテンツ管理部220からコンテンツ配信部230に提供される。コンテンツ管理部220は各種のコンテンツプロバイダからコンテンツを受領して、価格情報、コピー制限等の付帯情報(メタ情報)を付加し、所定の暗号化処理、署名処理を実行して、コンテンツ配信部230に提供する。

【0065】サービス管理センタ300は、コンテンツの暗号処理鍵の鍵管理センタとしての機能を有する。さらに、ユーザサイト100におけるコンテンツ利用状況に応じてセキュアモジュール115がメタ情報に基づいて生成する課金ログを収集する処理も実行する。セキュアモジュール115を持つユーザはサービス管理センタ300との間で、コンテンツ利用に応じた料金についてサービス管理センタ300が指定決済機関により決済処理を行なう旨の契約を結んでいる。また、サービス管理センタ300は、必要に応じて、更新された鍵をユーザサイト100のデータ処理手段110に送信する。

【0066】なお、サービス管理センタ300とユーザサイト100のデータ処理手段110との間のデータ通信の際には相互認証処理が実行され、相互認証の成立を条件として各種のデータが相互認証において生成したセッション鍵で暗号化されて送受信される。相互認証は例えば公開鍵暗号方式を適用して実行される。公開鍵暗号方式の認証時に用いられる公開鍵証明書は認証局400によって発行される。セキュアモジュール115には、公開鍵、秘密鍵の鍵ペア、認証局400によって発行された公開鍵証明書等が格納される。認証局400は、サービス管理センタ300、コンテンツ管理配信サイト200に対しても公開鍵証明書を発行する。

【0067】データ処理手段110の構成を図8に示す。データ処理手段110は、セットトップボックス等の受信手段からの入力データについての署名検証処理、各種鍵、コンテンツの復号処理を実行する。また、サービス管理センタとの通信を実行して、コンテンツ復号に適用する鍵を受領し、コンテンツ利用時に生成するコンテンツ利用情報を記録した課金ログをサービス管理センタに送信する処理等を実行する。サービス管理センタは、課金ログに基づいて予めユーザとの契約において設定された決済機関からコンテンツ利用料金の決済処理を行なう。

【0068】図8に示すデータ処理手段110の構成中、CPU(Central processing Unit)101は、データ処理手段内で実行されるプログラムの実行制御を行ない、RAM、ROM等のデータ記憶手段、およびセキュアモジュール115として構成された暗号処理部間のデータ転送制御、通信I/F105、106を介したデータ転送制御処理を実行する。

【0069】ROM(Read-Only-Memory)102は、例えばCPU101が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM(Random Access Memory)103は、CPU101の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0070】HDD104はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラム

の格納処理および読み出し処理を実行する。

【0071】セキュアモジュール115、いわゆるSAM(Secure Application Module)によって構成される暗号処理部は、例えば外部から入力される暗号化コンテンツデータの復号処理、サービス管理センタからの鍵送信の際、あるいはログ情報のサービス管理センタに対する送信時の認証処理、暗号処理、署名検証等のデータの検証処理等を実行する。暗号/復号化部122は、これらの各種処理におけるデータの暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを実行する。内部メモリ123には、例えばセキュアモジュールに固有の識別子(ID)、暗号鍵等が格納される。制御部121は、セキュアモジュール115内の処理の制御、該部とのデータ転送制御等を実行する。

【0072】通信インタフェース(I/F)105は、セットトップボックス、受信器、TV、再生装置等、コンテンツを受信する装置、あるいはコンテンツを再生する装置に接続するインタフェースであり、例えばIEEE1394インタフェース機能を持つ。また、通信インタフェース(I/F)106は、サービス管理センタとの通信接続インタフェースであり、例えばインターネット接続インタフェースであり、鍵の送受信、課金ログの送信等に利用される。

【0073】【コンテンツ配信処理例1】コンテンツ配信処理例の詳細を図9を参照して説明する。本実施例に示すコンテンツ配信システムでは、配送鍵(Kd)およびサブ配送鍵(SubKd)を用いる。

【0074】図9においては、A. サービス管理センタ300における処理(a1)、(a2)、B. コンテンツ管理配信サイトにおける処理(b1)~(b5)、C. ユーザサイトにおける処理(c1)~(c4)を示している。各処理について、処理シーケンスに従って説明する。

【0075】まず、A. サービス管理センタ300は、配送鍵(Kd)501およびサブ配送鍵(SubKd)502を生成し、これらについての処理を実行する。サービス管理センタ300は、これらの鍵を乱数に基づいて生成する。サービス管理センタ300は、(a1)の処理として、サブ配送鍵(SubKd)502を、配送鍵(Kd)501で暗号化する処理を行なう。

【0076】暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、例えば代表的な共通鍵暗号アルゴリズムであるDES(Data Encryption Standard)が適用できる。さらに、安全性を増すためにDESアルゴリズムを3重にして処理を行なうトリプルDESを適用してもよい。DES暗号化処理では鍵長56ビットの鍵を適用し、トリプルDESでは112ビットの鍵長を持つ鍵を適用することになる。サービス管理センタ300は、適用する暗号化方式に応じた鍵長の配送鍵(Kd)501およびサブ配送鍵(SubKd)502

を生成する。

【0077】(a1)の処理の結果、配送鍵(Kd)で暗号化処理されたサブ配送鍵(SubKd)、すなわち、Enc[Kd(SubKd)]が生成される。ここでEnc[a(b)]は、bをaで暗号化したデータを示すものとする。暗号化サブ配送鍵Enc[Kd(SubKd)]は、コンテンツ管理配信サイト200に転送される。

【0078】また、配送鍵(Kd)501についても、コンテンツ管理配信サイト200に転送するが、通信路におけるデータ漏洩等の問題の発生を避けるため、(a2)の処理として、配送鍵(Kd)501の暗号化処理(DES)を実行してコンテンツ管理配信サイト200に転送する。この場合の暗号化鍵としては、例えばコンテンツ管理配信サイト200と、サービス管理センタ300間において相互認証処理を実行し、認証処理の際に生成するセッション鍵(Ks)を適用することができる。あるいは双方が共通に保有する共通鍵、またはパスワードを用いて暗号化、復号化処理を実行する構成としてもよい。

【0079】サービス管理センタ300は、さらに、配送鍵(Kd)501をコンテンツ利用ユーザとして契約したユーザサイト100に送付する。なお、この場合の鍵送付処理に際しては、コンテンツ管理配信サイト200と、ユーザサイト100のデータ処理手段間において相互認証処理を実行し、認証の成立を条件とし、認証処理の際に生成するセッション鍵を適用して配送鍵(Kd)を暗号化して送信することが好ましい。

【0080】次に、B.コンテンツ管理配信サイト200における処理について説明する。コンテンツ管理配信サイト200は、まず(b1)の処理として、コンテンツを暗号化するためのコンテンツ鍵(Kc)503を生成する。コンテンツ鍵は、乱数発生装置において発生した乱数に基づいて生成するものであり、コンテンツ毎に生成する。コンテンツ鍵による暗号化処理が例えばDES暗号化処理である場合は鍵長56ビットの鍵を生成してコンテンツ鍵とし、トリプルDESの場合は112ビットの鍵長を持つ鍵をコンテンツ鍵として生成する。

【0081】次に、コンテンツ管理配信サイト200は、(b2)の処理として、生成したコンテンツ鍵(Kc)を用いてコンテンツの暗号化処理を実行する。暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、DES(Data Encryption Standard)、またはトリプルDESが適用できる。この暗号化処理の結果、暗号化コンテンツ:Enc[Kc(Content)]511が生成される。

【0082】さらに、コンテンツ管理配信サイト200は、(b3)の処理として、サービス管理センタ300から受信した暗号化されたサブ配送鍵データ:Enc[Ks(SubKd)]をセッション鍵Ksで復号し、

サブ配送鍵(SubKd)502を取得する。

【0083】次に、コンテンツ管理配信サイト200は、(b4)の処理として、取得したサブ配送鍵(SubKd)502を用いて、コンテンツ鍵(Ks)の暗号化処理を実行して暗号化コンテンツ鍵データ:Enc[SubKd(Kc)]512を生成する。

【0084】次に、コンテンツ管理配信サイト200は、暗号化コンテンツ鍵データ:Enc[SubKd(Kc)]512と、価格情報、コピー制限情報等の各種のコンテンツ関連利用情報からなるメタデータ521との双方のデータ、すなわち、(Enc[SubKd(Kc)]+メタデータ)からハッシュ(Hash)値を計算し、コンテンツ管理配信サイト200の秘密鍵(Ks)を用いた署名生成処理(b5)を実行する。署名生成処理は、例えば楕円曲線暗号方式の署名アルゴリズムであるECC-DSAに従って実行される。

【0085】コンテンツ管理配信サイト200は、上述の処理によって生成した暗号化コンテンツ:Enc[Kc(Content)]511、署名処理を施した暗号化コンテンツ鍵:Enc[SubKd(Kc)]512とメタデータ521、および、サービス管理センタ300から受信した暗号化サブ配送鍵:Enc[Kd(SubKd)]513、さらに、コンテンツ管理配信サイト200の公開鍵(Kp)を格納した公開鍵証明書をユーザサイトに向けて配信する。

【0086】次に、上記各データを受信するユーザサイト100における処理について説明する。ユーザサイト100では、通信衛星またはインターネット等の通信手段を介して例えばセットトップボックス等の受信手段120においてデータ受信を行ない、受信データをデータ処理手段110に転送する。受信データは、データ処理手段110の例えばハードディスク等の記憶手段に一旦格納される。

【0087】図9では、これらの格納データに対する処理手順を(c1)~(c4)として示している。まず、ユーザサイト100では、(c1)の処理として、コンテンツ管理配信サイト200から受信した署名処理を施した暗号化コンテンツ鍵:Enc[SubKd(Kc)]512とメタデータ521の署名検証処理を実行する。署名検証処理は、署名を、受信した公開鍵証明書から取り出したコンテンツ管理配信サイト200の公開鍵により解いた復号値と、受信データである(Enc[SubKd(Kc)]+メタデータ)からハッシュ(Hash)値を計算した結果とが一致するかどうかによって実行される。一致していた場合は、署名が正しく、データ、すなわち、受信データである(Enc[SubKd(Kc)]+メタデータ)の改ざんがないと判定され、次の処理ステップの実行が許可される。署名検証において両データが一致しなかった場合は、データ改ざんの可能性があると判定されて、次の処理が実行されず、処

理は終了する。

【0088】署名検証に成功すると、次に、ユーザサイト100では、(c2)の処理として、コンテンツ管理配信サイト200から受信した暗号化サブ配信鍵:  $Enc[K_d(SubK_d)]$  513を、サービス管理センタ300から受信した配信鍵( $K_d$ ) 501を用いて復号処理を実行し、サブ配信鍵( $SubK_d$ ) 502を取得する。

【0089】次に、ユーザサイト100では、(c3)の処理として、コンテンツ管理配信サイト200から受信した暗号化コンテンツ鍵:  $Enc[SubK_d(K_c)]$  512を、先の(c1)の処理で取得したサブ配信鍵( $SubK_d$ ) 502を用いて復号処理を実行し、コンテンツ鍵( $K_c$ ) 503を取得する。この復号処理の実行対象は、署名対象データ中に格納された暗号化コンテンツ鍵:  $Enc[SubK_d(K_c)]$  512である。

【0090】次に、ユーザサイト100では、(c4)の処理として、コンテンツ管理配信サイト200から受信した暗号化コンテンツ:  $Enc[K_c(Content)]$  511を、先の(c2)の処理で取得したコンテンツ鍵( $K_c$ ) 503を用いて復号処理を実行し、コンテンツ( $Content$ ) 520を取得する。

【0091】取得したコンテンツは、データ処理手段110のインタフェースを介して接続されたセットトップボックス、または再生手段としてのTVに転送され再生される。

【0092】上述した処理において、コンテンツ管理配信サイト200は、暗号化コンテンツ鍵:  $Enc[SubK_d(K_c)]$  512とメタデータ521の双方のデータからハッシュ(Hash)値を計算して、コンテンツ管理配信サイトの秘密鍵( $K_s$ )で署名処理を施す。ユーザサイト100で実行する署名検証処理は、受信データである( $Enc[SubK_d(K_c)]$  + メタデータ)に対する署名検証として実行されることになるので、署名対象データに含まれる暗号化コンテンツ鍵を他のコンテンツのものに置きかえると署名検証処理に失敗して、後続ステップの実行が許可されない。従って、コンテンツ鍵の取得、コンテンツの復号が不可能になり、不正なコンテンツの利用は排除されることになる。また、メタデータに基づいて生成される課金ログデータも、正しいコンテンツに対応するものとなり、正しい課金処理が実行される。

【0093】【コンテンツ配信処理例2】次に、第2のコンテンツ配信処理例として、サービス管理センタからユーザサイトに対して配信鍵( $K_d$ )を送信することなく、各ユーザに予めユーザ毎の個別鍵を渡し、コンテンツ管理配信サイトが各個別鍵で暗号化した配信鍵を暗号化コンテンツとともにユーザサイトに配信するシステム構成例について図10を参照して説明する。

【0094】本例のコンテンツ配信システムでは、サブ配信鍵( $K_d$ )および個別鍵( $K_i$ )を用いる。ただし  $i=1 \sim n$  であり、各々が異なる鍵である。この個別鍵( $K_i$ )は、契約ユーザに対してサービス管理センタが例えばセキュアモジュール構造を持つICカードに個別鍵( $K_i$ )を内蔵して契約ユーザに付与または貸与する。ユーザは、個別鍵( $K_i$ )を内蔵したICカードをデータ処理手段110(図7、図8参照)にセットして、個別鍵( $K_i$ )を適用した処理を実行する。例えば図8のデータ処理手段構成において、セキュアモジュール115がデータ処理手段110に対して着脱可能なICカードとして構成される。

【0095】図10を参照して本実施例におけるコンテンツ配信処理のシーケンスを説明する。図10には、前述の実施例1と同様、A. サービス管理センタ300における処理(a1)。(a2)、B. コンテンツ管理配信サイトにおける処理(b1)～(b5)、C. ユーザサイトにおける処理(c1)～(c4)を示している。各処理について説明する。

【0096】まず、A. サービス管理センタ300は、個別鍵( $K_i$ ) 601およびサブ配信鍵( $SubK_d$ ) 602を生成し、これらについての処理を実行する。個別鍵( $K_i$ )は、契約ユーザの数に応じて契約ユーザ毎に生成するものであり、契約ユーザに対して例えばICカード等のモジュールに格納して配布した後は、A. サービス管理センタ300において同一の鍵を保持管理する。また、サブ配信鍵( $SubK_d$ )は、配信コンテンツ毎に生成、あるいは定期的に更新する鍵として設定する。サービス管理センタ300は、これらの鍵を乱数に基づいて生成する。サービス管理センタ300は、(a1)の処理として、各個別鍵( $K_i$ ) 601を用いて、サブ配信鍵( $SubK_d$ ) 602を暗号化する処理を行なう。A. サービス管理センタ300は、契約ユーザ数に応じて生成済みの  $n$  個の個別鍵( $k_i$ ) 601 ( $i=1 \sim n$ )を適用してサブ配信鍵( $SubK_d$ ) 602を暗号化し、 $n$  個の暗号化サブ配信鍵:  $Enc[K_i(SubK_d)]$  を生成する。

【0097】暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、例えば代表的な共通鍵暗号アルゴリズムであるDES(Data Encryption Standard)が適用できる。さらに、安全性を増すためにDESアルゴリズムを3重にして処理を行なうトリプルDESを適用してもよい。DES暗号化処理では鍵長56ビットの鍵を適用し、トリプルDESでは112ビットの鍵長を持つ鍵を適用することになる。サービス管理センタ300は、適用する暗号化方式に応じた鍵長の個別鍵( $K_i$ ) 601およびサブ配信鍵( $SubK_d$ ) 602を生成する。

【0098】(a1)の処理の結果、 $n$  個の個別鍵( $K_i$ )で暗号化処理されたサブ配信鍵( $SubK_d$ )、す

なわち、 $Enc[K_i(SubKd)]$  ( $i=1\sim n$ ) が生成される。 $n$ 個の暗号化サブ配送鍵 $Enc[K_i(SubKd)]$ は、コンテンツ管理配信サイト200に転送される。

【0099】また、サブ配送鍵( $SubKd$ )602についても、コンテンツ管理配信サイト200に転送するが、通信路におけるデータ漏洩等の問題の発生を避けるため、(a2)の処理として、サブ配送鍵( $SubKd$ )602の暗号化処理(DES)を実行してコンテンツ管理配信サイト200に転送する。この場合の暗号化鍵としては、例えばコンテンツ管理配信サイト200と、サービス管理センタ300間において相互認証処理を実行し、認証処理の際に生成するセッション鍵( $Ks$ )を適用することができる。あるいは双方が共通に保有する共通鍵、またはパスワードを用いて暗号化、復号化処理を実行する構成としてもよい。

【0100】次に、B. コンテンツ管理配信サイト200における処理について説明する。コンテンツ管理配信サイト200は、まず(b1)の処理として、コンテンツを暗号化するためのコンテンツ鍵( $Kc$ )603を生成する。コンテンツ鍵は、乱数発生装置において発生した乱数に基づいて生成するものであり、コンテンツ毎に生成する。コンテンツ鍵による暗号化処理が例えばDES暗号化処理である場合は鍵長56ビットの鍵を生成してコンテンツ鍵とし、トリプルDESの場合は112ビットの鍵長を持つ鍵をコンテンツ鍵として生成する。

【0101】次に、コンテンツ管理配信サイト200は、(b2)の処理として、生成したコンテンツ鍵( $Kc$ )を用いてコンテンツの暗号化処理を実行する。暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、DES(Data Encryption Standard)、またはトリプルDESが適用できる。この暗号化処理の結果、暗号化コンテンツ: $Enc[Kc(Content)]$ 611が生成される。

【0102】さらに、コンテンツ管理配信サイト200は、(b3)の処理として、サービス管理センタ300から受信した暗号化されたサブ配送鍵データ: $Enc[Ks(SubKd)]$ をセッション鍵 $Ks$ で復号し、サブ配送鍵( $SubKd$ )602を取得する。

【0103】次に、コンテンツ管理配信サイト200は、(b4)の処理として、取得したサブ配送鍵( $SubKd$ )602を用いて、コンテンツ鍵( $Ks$ )の暗号化処理を実行して暗号化コンテンツ鍵データ: $Enc[SubKd(Kc)]$ 612を生成する。

【0104】次に、コンテンツ管理配信サイト200は、暗号化コンテンツ鍵データ: $Enc[SubKd(Kc)]$ 612と、価格情報、コピー制限情報等の各種のコンテンツ関連利用情報からなるメタデータ621との双方のデータ、すなわち、( $Enc[SubKd(Kc)]$ +メタデータ)からハッシュ(Hash)値

を計算し、コンテンツ管理配信サイト200の秘密鍵( $Ks$ )を用いた署名生成処理(b5)を実行する。署名生成処理は、例えば楕円曲線暗号方式の署名アルゴリズムであるECC-DSAに従って実行される。

【0105】コンテンツ管理配信サイト200は、上述の処理によって生成した暗号化コンテンツ: $Enc[Kc(Content)]$ 611、署名処理を施した暗号化コンテンツ鍵: $Enc[SubKd(Kc)]$ 612とメタデータ621、および、サービス管理センタ300から受信した暗号化サブ配送鍵: $Enc[Ki(SubKd)]$ 613、さらに、コンテンツ管理配信サイト200の公開鍵( $Kp$ )を格納した公開鍵証明書をユーザサイトに向けて配信する。

【0106】なお、従来技術の欄で説明したCAS(Conditional Access System)において、本実施例の構成を適用することが可能であり、この場合には、コンテンツ管理配信サイト200からユーザサイト100に対して送信する署名処理を施した暗号化コンテンツ鍵: $Enc[SubKd(Kc)]$ 612とメタデータ621は、コンテンツ番組情報を含むECM(Entitlement Control Message)内に含ませて放送データとして送信する。また、コンテンツ管理配信サイト200からユーザサイト100に対して送信する暗号化サブ配送鍵: $Enc[Ki(SubKd)]$ 613は、各ユーザに渡されているICカードの識別子(ID)を付加情報として持つEMM(Entitlement Management Message)に含ませて放送波で送信する。

【0107】次に、上記各データを受信するユーザサイト100における処理について説明する。ユーザサイト100では、通信衛星またはインターネット等の通信手段を介して例えばセットトップボックス等の受信手段120においてデータ受信を行ない、受信データをデータ処理手段110に転送する。受信データは、データ処理手段110の例えばハードディスク等の記憶手段に一旦格納される。

【0108】図10では、これらの格納データに対する処理手順を(c1)~(c4)として示している。まず、ユーザサイト100では、(c1)の処理として、コンテンツ管理配信サイト200から受信した署名処理を施した暗号化コンテンツ鍵: $Enc[SubKd(Kc)]$ 612とメタデータ621の署名検証処理を実行する。署名検証処理は、署名を、受信した公開鍵証明書から取り出したコンテンツ管理配信サイト200の公開鍵を適用して解いた復号値と、受信データである( $Enc[SubKd(Kc)]$ +メタデータ)からハッシュ(Hash)値を計算した結果とが一致するかどうかによって実行される。一致していた場合は、署名が正しく、データ、すなわち、受信データである( $Enc[SubKd(Kc)]$ +メタデータ)の改竄がないと判定され、次の処理ステップの実行が許可される。署名検証に

において両データが一致しなかった場合は、データ改竄の可能性があると判定されて、次の処理が実行されず、処理は終了する。

【0109】署名検証に成功すると、次に、ユーザサイト100では、(c2)の処理として、コンテンツ管理配信サイト200から受信した暗号化サブ配送鍵:  $Enc[K_i(SubKd)]$  613を、サービス管理センタ300から予め受領済みの個別鍵( $K_i$ ) 601を用いて復号処理を実行し、サブ配送鍵( $SubKd$ ) 602を取得する。

【0110】コンテンツ管理配信サイト200から受信する暗号化サブ配送鍵:  $Enc[K_i(SubKd)]$  613は、ユーザ数に応じた1~nの各個別鍵で暗号化したサブ配送鍵のデータである。コンテンツ管理配信サイト200から受信する暗号化サブ配送鍵:  $Enc[K_i(SubKd)]$  ( $i=1\sim n$ )には各データ毎に識別データが付与されており、この識別データは、各ユーザに渡されているICカードの識別子(ID)に対応するものとなっている。ユーザサイトのデータ処理手段のセキュアモジュール(ICカード)では、自己のICカードに一致するIDを持つ暗号化サブ配送鍵:  $Enc[K_i(SubKd)]$  データの選択処理を実行して、選択された暗号化サブ配送鍵:  $Enc[K_i(SubKd)]$  に対して、ICカードに格納された個別鍵( $K_i$ )を適用した復号処理を実行してサブ配送鍵( $SubKd$ )を取得する。

【0111】次に、ユーザサイト100では、(c3)の処理として、コンテンツ管理配信サイト200から受信した暗号化コンテンツ鍵:  $Enc[SubKd(Kc)]$  612を、先の(c1)の処理で取得したサブ配送鍵( $SubKd$ ) 602を用いて復号処理を実行し、コンテンツ鍵( $Kc$ ) 603を取得する。この復号処理の実行対象は、署名対象データ中に格納された暗号化コンテンツ鍵:  $Enc[SubKd(Kc)]$  612である。

【0112】次に、ユーザサイト100では、(c4)の処理として、コンテンツ管理配信サイト200から受信した暗号化コンテンツ:  $Enc[Kc(Content)]$  611を、先の(c2)の処理で取得したコンテンツ鍵( $Kc$ ) 603を用いて復号処理を実行し、コンテンツ( $Content$ ) 620を取得する。

【0113】取得したコンテンツは、データ処理手段110のインタフェースを介して接続されたセットトップボックス、または再生手段としてのTVに転送され再生される。

【0114】上述した処理例においても、コンテンツ管理配信サイト200は、暗号化コンテンツ鍵:  $Enc[SubKd(Kc)]$  612とメタデータ621の双方のデータからハッシュ(Hash)値を計算して、コンテンツ管理配信サイトの秘密鍵( $Ks$ )で署名処理を施

す。ユーザサイト100で実行する署名検証処理は、受信データである( $Enc[SubKd(Kc)]$  + メタデータ)に対する署名検証として実行されることになるので、署名対象データに含まれる暗号化コンテンツ鍵を他のコンテンツのものに置きかえると署名検証処理に失敗して、後続ステップの実行が許可されない。従って、コンテンツ鍵の取得、コンテンツの復号が不可能になり、不正なコンテンツの利用は排除されることになる。また、メタデータに基づいて生成される課金ログデータも、正しいコンテンツに対応するものとなり、正しい課金処理が実行される。

【0115】個別鍵( $K_i$ ) 601は、コンテンツ管理配信サイト200から正規なユーザサイト100にのみ安全なセキュアモジュール(例えばICカード)に格納されて配布され、正規なユーザサイト100において管理されることにより、漏洩は防止される。

【0116】このように、本発明のシステムにおいては、個別鍵( $K_i$ )を、コンテンツの配信を行なう例えば放送局のようなコンテンツ管理配信サイトに渡すことなく、暗号化コンテンツ配信が実現され、コンテンツ管理配信サイトにおける個別鍵( $K_i$ )の安全管理体制を強いることなく鍵の漏洩が防止され、コンテンツの保護構成が実現されることになる。

【0117】[メタデータおよびコンテンツ鍵に対する署名処理] 図11に、本発明の構成において実行される電子署名の検証に基づくコンテンツ(番組)再生の各種態様について説明する図を示す。

【0118】図11(a)は、正しいコンテンツ利用態様、すなわち署名検証が成立(OK)し、コンテンツ(番組)再生が許可される場合の例である。コンテンツ管理配信サイトでは、価格情報を含むメタデータ、サブ配送鍵( $SubKd$ )で暗号化したコンテンツ鍵に対するハッシュ(Hash)値を計算し、秘密鍵( $Ks$ )を用いて署名を生成し、ユーザサイトに送信する。なお、サブ配送鍵( $SubKd$ )は、配送鍵( $Kd$ )または、個別鍵( $K_i$ )によって暗号化された暗号化サブ配送鍵としてユーザサイトに送信される。

【0119】ユーザサイトでは、暗号化サブ配送鍵を配送鍵( $Kd$ )または、個別鍵( $K_i$ )によって復号し、サブ配送鍵( $SubKd$ )を取得し、コンテンツ(番組A)に対応するコンテンツ鍵( $Kc-a$ )を暗号化している配送鍵( $Kd$ )を、取得したサブ配送鍵( $SubKd$ )で復号することにより取得して、さらに、配送鍵( $Kd$ )に基づいて暗号化コンテンツ鍵の復号処理を実行することにより、コンテンツ鍵( $Kc-a$ )を取得し、取得したコンテンツ鍵( $Kc-a$ )で暗号化コンテンツの復号を行なってコンテンツを再生利用することができる。

【0120】しかし、図9、図10を用いて説明したように、配送鍵( $Kd$ )または、個別鍵( $K_i$ )によって

暗号化された暗号化サブ配送鍵の復号処理の実行条件として、署名の検証に成功することが設定されている。

【0121】図11(a)の場合は、番組Aに対するメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に対してハッシュ値が計算されて署名がなされ、ユーザサイトは署名検証をコンテンツ管理配信サイトの公開鍵証明書から取り出した公開鍵を用いて実行する。番組Aに対するメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値は、データの改竄、置き換えがなされていないので、一致することになる。従って、次のステップとして、配送鍵(kd)または、個別鍵(Ki)によって暗号化された暗号化サブ配送鍵の復号処理が実行され、さらに後続処理(図9、10における(c2)~(c4))を実行して、コンテンツの再生が可能となる。

【0122】図11(b)の場合は、番組Aに対するメタデータが改竄された場合を示している。例えば本来コンテンツ(番組A)の価格が300円と記録されていたものを100円と改竄したとする。この場合、ユーザサイトで実行される署名検証処理は、改竄されたメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値との比較として実行される。この比較処理においては、データの一致は得られないことになる。署名は、改竄されたメタデータと異なる番組Aの本来のメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に基づいて計算したハッシュ値に対してなされたものであるからである。従って、署名検証成立を条件として実行可能となる暗号化サブ配送鍵の復号処理が実行されず、さらに後続処理(図9、10における(c2)~(c4))も実行不可能となり、コンテンツの再生が不可能となる。

【0123】図11(c)の場合は、番組Aに対するメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に対する署名検証を実行し、署名検証の成立に基づいて、他のコンテンツ(番組B)の利用を行なおうとする例である。すなわち、メタデータと署名との置き換え処理によって他のコンテンツの不正利用を実行しようとした場合の処理例である。この場合、ユーザサイトで実行される署名検証処理は、番組Aのメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値との比較として実行され、この比較処理においてデータの一致が得られる。従って、次のステップとして、配送鍵(kd)または、個別鍵(Ki)によって暗号化された暗号化サブ配送鍵の復号処理が実行される。しかし、取得したサブ配送鍵によって復号取得可能なコンテンツ鍵は、署名検証に成功した番組Aに対するコンテンツ鍵(Kc-a)であり、他のコンテンツ(例

えば番組B)のコンテンツ鍵ではない。署名検証成立を条件として取得されるコンテンツ鍵は、署名対象データに含まれるコンテンツ鍵であり、他のコンテンツの復号は防止され、コンテンツの不正利用が排除される。

【0124】図12に、本発明の署名検証処理を条件とするコンテンツ利用処理について説明する図を示す。コンテンツ管理配信サイトでは、価格情報を含むメタデータ、サブ配送鍵(SubKd)で暗号化したコンテンツ鍵に対するハッシュ(Hash)値を計算し、秘密鍵(Ks)を用いて署名を生成し、ユーザサイトに送信する。なお、サブ配送鍵(SubKd)は、配送鍵(kd)または、個別鍵(Ki)によって暗号化された暗号化サブ配送鍵としてユーザサイトに送信する。

【0125】ユーザサイトは署名検証をコンテンツ管理配信サイトの公開鍵証明書から取り出した公開鍵を用いて実行する。具体的には、番組Aに対するメタデータと番組Aの暗号化コンテンツ鍵(Kc-a)に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値との比較処理を行なう。署名対象データの改竄、置き換えがなされていない場合は、一致することになる。一致したことを条件として、次のステップの実行が許可される。すなわち、配送鍵(kd)または、個別鍵(Ki)によって暗号化された暗号化サブ配送鍵の復号処理が実行され、さらに後続処理、コンテンツ(番組A)に対応するコンテンツ鍵(Kc-a)を暗号化している配送鍵(Kd)を、取得したサブ配送鍵(SubKd)で復号することにより取得して、さらに、配送鍵(Kd)に基づいて暗号化コンテンツ鍵の復号処理を実行することにより、コンテンツ鍵(Kc-a)を取得し、取得したコンテンツ鍵(Kc-a)で暗号化コンテンツの復号を行なってコンテンツを再生利用することができる。この一連の処理で取得されるコンテンツ鍵は、署名対象データ無いに格納されたコンテンツ鍵に限られ、他のコンテンツ(番組B)の復号に適用することはできない。

【0126】次に、本発明のコンテンツ配信システムにおける処理手順について図13に示すフローを用いて説明する。まず、ステップS301において、コンテンツ管理配信サイトは、コンテンツを暗号化するためのコンテンツ鍵(Kc)を、例えば乱数発生装置において発生した乱数に基づいて生成し、コンテンツ鍵によるコンテンツ(番組)の暗号化処理を実行する。暗号化処理が例えばDES暗号化処理である場合は鍵長56ビットのコンテンツ鍵とし、トリプルDESの場合は112ビットの鍵長を持つ鍵をコンテンツ鍵を適用する。

【0127】次に、ステップS302において、コンテンツ管理配信サイトは、サブ配送鍵(SubKd)を用いて、コンテンツ鍵(Ks)の暗号化処理を実行して暗号化コンテンツ鍵データ: Enc[SubKd(Kc)]を生成する。



【0128】次に、ステップS303において、コンテンツ管理配信サイトは、暗号化コンテンツ鍵データと、価格情報、コピー制限情報等の各種のコンテンツ関連利用情報からなるメタデータとの双方のデータ、すなわち、 $(Enc[SubKd(Kc)] + \text{メタデータ})$  からハッシュ (Hash) 値を計算し、コンテンツ管理配信サイトの秘密鍵 ( $K_s$ ) を用いた署名生成処理を実行する。署名生成処理は、例えば楕円曲線暗号方式の署名アルゴリズムである ECC-DSA に従って実行される。

【0129】コンテンツ管理配信サイトは、ステップS304で、生成した暗号化コンテンツ:  $Enc[Kc(Conte nt)]$ 、署名処理を施した暗号化コンテンツ鍵:  $Enc[SubKd(Kc)]$  とメタデータをユーザサイトに向けて配信する。なお、必要であればコンテンツ管理配信サイトの公開鍵証明書も併せて送付する。

【0130】以下のステップS305以下の処理はユーザサイトにおける処理である。なお、ステップS321は、署名対象データであるメタデータ+暗号化コンテンツ鍵の改竄を実行した場合 (図11(b)に相当)、ステップS322は、署名対象データであるメタデータ+暗号化コンテンツ鍵の置き換えを実行した場合 (図11(c)に相当) を示している。

【0131】ユーザサイトでは、コンテンツ管理配信サイトから受信した署名処理を施した暗号化コンテンツ鍵:  $Enc[SubKd(Kc)]$  とメタデータの署名検証処理を実行する。まず、ステップS305において、受信データである  $(Enc[SubKd(Kc)] + \text{メタデータ})$  からハッシュ (Hash) 値を計算する。この取得値を①とする。次にステップS306において、受信した署名を、コンテンツ管理配信サイトの公開鍵を適用して解き、値を取得する。この取得値を②とする。

【0132】ステップS307では、上記取得値①、②の比較を実行する。一致していない場合は、署名検証に失敗と判定され、以下の処理は実行されず、処理は終了する。ステップS321におけるデータ改竄、ステップS307において不一致 (false) となり、処理が終了となり、コンテンツは再生されない。

【0133】ステップS307で署名検証に成功 (true) した場合は、ステップS308に進み、コンテンツ管理配信サイトから受信した暗号化サブ配送鍵:  $Enc[Kd(SubKd)]$  を、配送鍵 ( $K_d$ ) または個別鍵 ( $K_i$ ) を用いて復号し、サブ配送鍵 ( $SubK_d$ ) を取得する。

【0134】次に、ステップS309では、コンテンツ管理配信サイトから受信した暗号化コンテンツ鍵:  $Enc[SubKd(Kc)]$  を、先の処理で取得したサブ配送鍵 ( $SubK_d$ ) を用いて復号し、コンテンツ鍵

( $K_c$ ) を取得する。

【0135】次に、ステップS310において、取得したコンテンツ鍵 ( $K_c$ ) が再生対象コンテンツ (番組) のコンテンツ鍵として適用できるかを判定する。正当なデータに対して署名検証処理が実行されていれば、取得したコンテンツ鍵 ( $K_c$ ) は、再生対象コンテンツ (番組) のコンテンツ鍵として適用できる。しかし、ステップS322におけるデータ置き換えが行われた場合は、署名検証の結果後の一連の処理によって取得されるコンテンツ鍵 ( $K_c$ ) は、再生対象コンテンツ (番組) のコンテンツ鍵として適用できない。従って、この時点で処理は終了する。

【0136】取得したコンテンツ鍵 ( $K_c$ ) が、再生対象コンテンツ (番組) のコンテンツ鍵である場合は、ステップS311において、コンテンツ管理配信サイトから受信した暗号化コンテンツ:  $Enc[Kc(Conte nt)]$  を、取得したコンテンツ鍵 ( $K_c$ ) を用いて復号し、コンテンツ (Content) を取得し、ステップS312において、コンテンツ (番組) を再生する。さらに、ステップS313において、署名検証処理の対象データ中に含まれるメタデータに記録された価格情報に基づいて課金情報を生成し、サービス管理センターに送信する。

【0137】[各エンティティの構成] 次に、上述したコンテンツ配信システムを構成する各エンティティ、すなわち、サービス管理センタおよびコンテンツ管理配信サイトの構成例について図14を参照して説明する。

【0138】サービス管理センタおよびコンテンツ管理配信サイトは他エンティティと通信可能な通信手段を備えたデータ処理手段によって実現することができる。図14にシステム構成例を示す。なお、図14に示すシステム構成例は1つの例であり、各システムは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。図14に示すCPU (Central processing Unit) 701は、各種アプリケーションプログラムや、OS (Operating System) を実行するプロセッサである。ROM (Read-Only-Memory) 702は、CPU 701が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM (Random Access Memory) 703は、CPU 701の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0139】HDD 704はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。暗号処理手段705は、送信データの暗号処理、復号処理、署名生成、検証処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをROM 702に格納し、CPU 701がR

OM格納プログラムを読み出して実行するように構成してもよい、メモリ（セキュアモジュール）706は例えば耐タンパ構造を持つメモリとして構成され、暗号処理に必要な鍵データ、アクセス許可書の格納領域として使用可能である。なお、これらのデータは、他のメモリ領域、記憶媒体に格納することも可能である。

【0140】バス721はPCI（Peripheral Components Interconnect）バス等により構成され、各モジュール、入出力インタフェース722を介した各入力装置とのデータ転送を可能にしている。

【0141】入力部711は、例えばキーボード、ポインティングデバイス等によって構成され、CPU701に各種のコマンド、データを入力するためにユーザにより操作される。出力部712は、例えばCRT、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【0142】通信部713はデバイスの接続したエンティティ、例えばサービス管理センタまたはコンテンツ管理配信サイト、またはユーザサイト等との通信処理を実行し、CPU701の制御の下に、各記憶部から供給されたデータ、あるいはCPU701によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

【0143】ドライブ714は、フロッピー（登録商標）ディスク、CD-ROM（Compact Disc Read Only Memory）、MO（Magneto optical）ディスク、DVD（Digital Versatile Disc）、磁気ディスク、半導体メモリなどのリムーバブル記録媒体715の記録再生を実行するドライブであり、各リムーバブル記録媒体715からのプログラムまたはデータ再生、リムーバブル記録媒体715に対するプログラムまたはデータ格納を実行する。

【0144】各記憶媒体に記録されたプログラムまたはデータを読み出してCPU701において実行または処理を行なう場合は、読み出したプログラム、データは入出力インタフェース722、バス721を介して例えば接続されているRAM703に供給される。

【0145】先の説明内に含まれるサービス管理センタ、コンテンツ管理配信サイトにおける処理を実行するためのプログラムは例えばROM702に格納されてCPU701によって処理されるか、あるいはハードディスクに格納されHDD704を介してCPU701に供給されて実行される。

【0146】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0147】なお、明細書中において説明した一連の処

理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【0148】例えば、プログラムは記録媒体としてのハードディスクやROM（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM（Compact Disc Read Only Memory）、MO（Magneto optical）ディスク、DVD（Digital Versatile Disc）、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0149】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN（Local Area Network）、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【0150】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0151】

【発明の効果】以上、説明したように、本発明のコンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムによれば、暗号化コンテンツの配信を行ない、正規ユーザにおいてのみコンテンツの利用を許容しようとするシステムにおいて、コンテンツの配信を行なう例えば放送局のようなコンテンツ管理配信サイトにおいて、コンテンツの価格情報を含むメタデータと、コンテンツの暗号処理に適用するコンテンツ鍵を併せたデータのハッシュ値を生成して電子署名を実行し、データを受信したユーザサイトにおいて、署名検証の成立を条件として署名対象データ中に格納されたコンテンツ鍵の取得を可能とする構成としたので、メタデータの改竄、あるいはメタデータを含むデータの置き換えなどの不正な処理によるコンテンツの不正利用を防止することが可能となる。

【図面の簡単な説明】

【図 1】従来のコンテンツ配信システムの処理構成を説明する図である。

【図 2】従来のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。

【図 3】従来のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。

【図 4】従来のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。

【図 5】従来のコンテンツ配信システムにおけるメタデータの置き換えによるコンテンツ不正利用について説明するフロー図である。

【図 6】従来のコンテンツ配信システムにおける署名検証に基づくコンテンツ利用について説明するフロー図である。

【図 7】本発明のコンテンツ配信システムの概要を説明するブロック図である。

【図 8】本発明のコンテンツ配信システムのユーザサイトに構成されるデータ処理装置の構成例を示すブロック図である。

【図 9】本発明のコンテンツ配信システムのコンテンツ配信処理例（実施例 1）を示す図である。

【図 10】本発明のコンテンツ配信システムのコンテンツ配信処理例（実施例 2）を示す図である。

【図 11】本発明のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。

【図 12】本発明のコンテンツ配信システムにおける署名検証に基づくコンテンツ利用について説明する図である。

【図 13】本発明のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明するフロー図である。

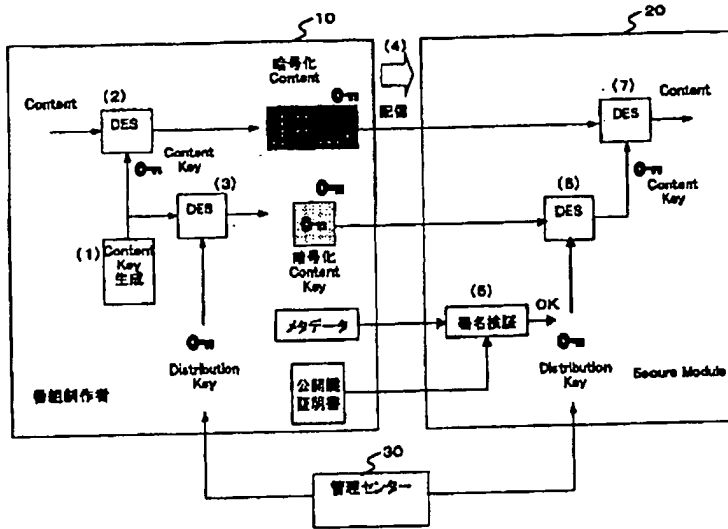
【図 14】本発明のコンテンツ配信システムのサービス管理センタ、コンテンツ管理配信サイトのシステム構成例を示す図である。

【符号の説明】

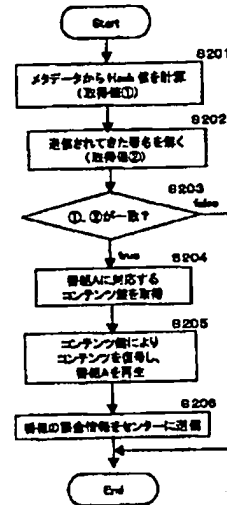
- 10 コンテンツ提供サイト
- 20 ユーザサイト
- 30 管理センター
- 100 ユーザサイト
- 110 データ処理手段
- 115 セキュアモジュール
- 120 受信手段

- 140 出力手段
- 200 コンテンツ管理配信サイト
- 220 コンテンツ管理部
- 230 コンテンツ配信部
- 300 サービス管理センタ
- 400 認証局
- 101 CPU (Central processing Unit)
- 102 ROM (Read-Only-Memory)
- 103 RAM (Random Access Memory)
- 104 HDD
- 105, 106 通信 I/F
- 121 制御部
- 122 暗号/復号化部
- 123 内部メモリ
- 501 配送鍵
- 502 サブ配送鍵
- 503 コンテンツ鍵
- 511 暗号化コンテンツ
- 512 暗号化コンテンツ鍵
- 513 暗号化サブ配送鍵
- 520 コンテンツ
- 521 メタデータ
- 522 公開鍵証明書
- 601 個別鍵
- 602 サブ配送鍵
- 603 コンテンツ鍵
- 611 暗号化コンテンツ
- 612 暗号化コンテンツ鍵
- 613 暗号化サブ配送鍵
- 620 コンテンツ
- 621 メタデータ
- 622 公開鍵証明書
- 701 CPU (Central processing Unit)
- 702 ROM (Read-Only-Memory)
- 703 RAM (Random Access Memory)
- 704 HDD
- 705 暗号処理手段
- 706 メモリ (セキュアモジュール)
- 711 入力部
- 712 出力部
- 713 通信部
- 714 ドライブ
- 715 リムーバブル記録媒体
- 721 バス
- 722 入出力インタフェース

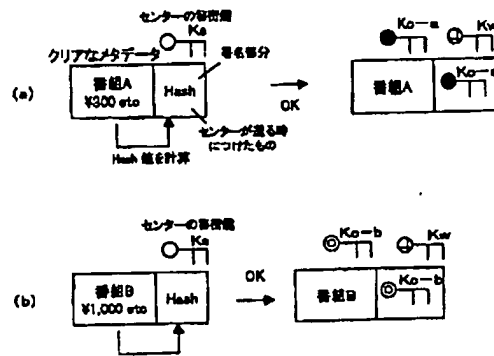
【図1】



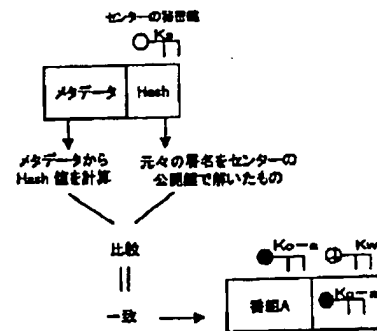
【図6】



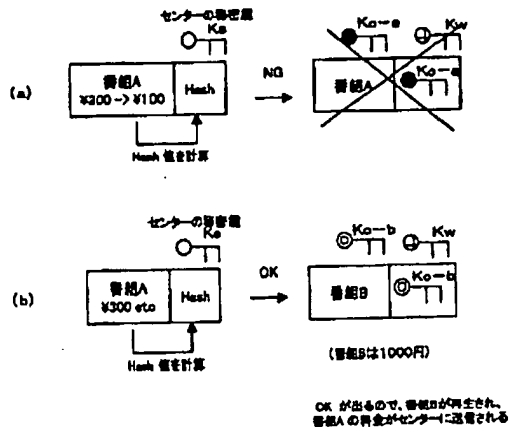
【図2】



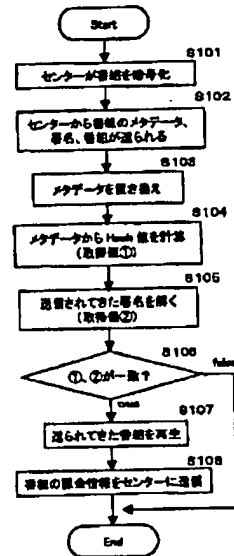
【図4】



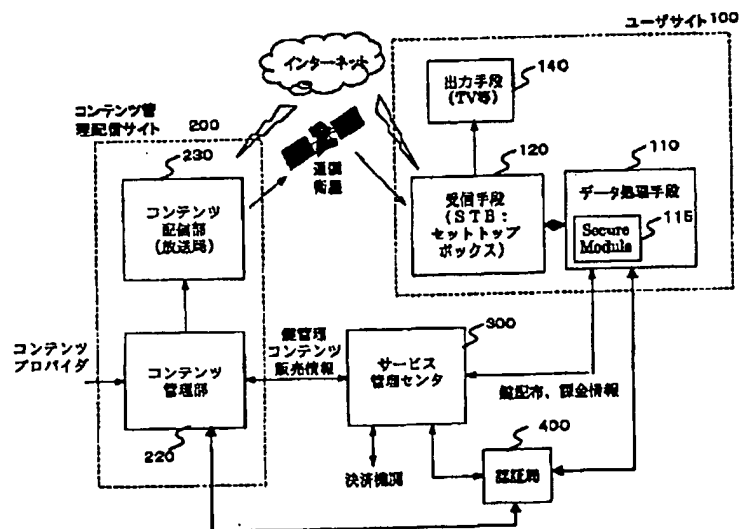
【図3】



【図5】



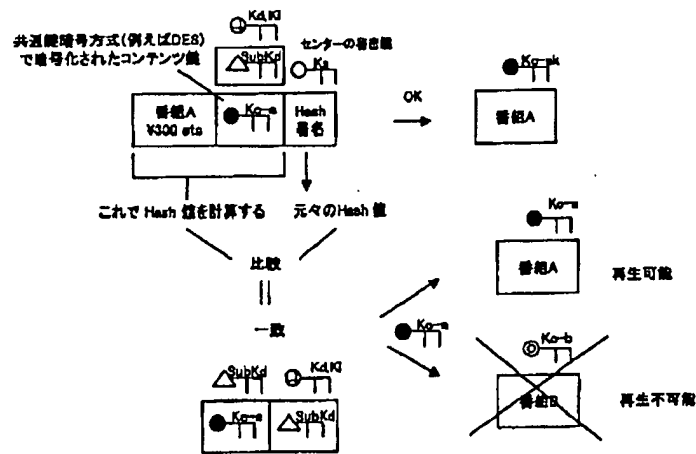
【図7】



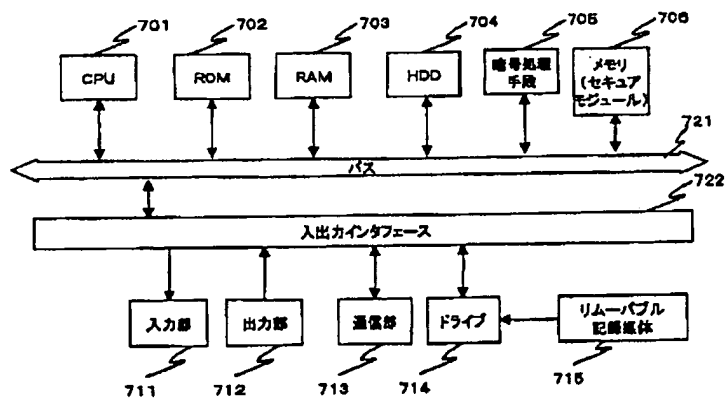




【図12】



【図14】



フロントページの続き

(51) Int. Cl.	識別記号	FI	コード (参考)
H04N 7/081		H04L 9/00	601A
7/16			601E
// H04N 7/167		H04N 7/08	Z
		7/167	Z



Fターム(参考) 5C063 AB03 AB07 AC01 AC05 AC10  
CA23 CA36 DA07 DA13 DB10  
5C064 BA01 BB01 BB02 B004 BC06  
BC17 BC18 BC22 BC23 BD02  
BD04 BD08 BD09 CA14 CB01  
CC01 CC04  
5J104 AA09 AA12 AA16 EA06 EA19  
LA06 NA02 NA12 PA11